Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-O-001**
Název dokumentu:	**Využívání prostředků anonymizace**
Typ dokumentu:	Opatření výboru pro řízení kybernetické bezpečnosti JU
Rozsah:	Rozsah opatření je specifikován v rámci dokumentu.
Prvek legislativy:	-----
Datum vydání:	25. 2. 2025
Datum účinnosti:	**1. 3. 2025**
Platnost do:	odvolání
Počet stran + příloh:	3 + 0
Verze:	1.0
Význam a benefity:	Význam opatření je upozornit uživatele na zásah Výboru KB JU proti anonymním VPN a proxy serverům. Opatření dále seznamuje uživatele s problematikou využívání prostředků anonymizace a jejich dopadu na služby JU a M365.
Uložení:	ISMS část na Wiki JU – wiki.jcu.cz
Ruší dokumenty:	-----
Zpracovatel:	Jan Urbánek - Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Zavedení opatření

Cílem tohoto opatření je informovat uživatele JU o zákazu využívání všech anonymizačních prostředků při komunikaci se službami JU a M365 společnosti Microsoft, které JU využívá.

Toto zahrnuje, ale není omezeno na, volně dostupné a komerční virtuální privátní sítě (VPN), proxy servery, anonymizační webové prohlížeče, peer-to-peer (P2P) sítě a další technologie sloužící k anonymizaci.

Reakce na využívání těchto nástrojů je nezbytná z následujících důvodů:

- **Redukce útočných vektorů**: Anonymizační prostředky jsou stále více zneužívány útočníky pro maskování jejich aktivit, což zvyšuje riziko kybernetických útoků cílených na JU.
- **Snížení falešných poplachů**: Anonymizační nástroje často generují síťový provoz, který je identifikován jako potenciální kybernetický útok. Tím vzniká množství falešných poplachů, které ztěžují efektivní správu bezpečnosti a odvádějí pozornost od skutečných hrozeb.

a) Rozsah působnosti opatření

Opatření se vztahuje na všechny zaměstnance JU, studenty a účastníky ČZV JU, dodavatele a jakékoli další osoby či subjekty využívající služby poskytované JU.

b) Zakázané anonymizační prostředky

Používání následujících anonymizačních nástrojů bude napříč JU vyhodnoceno jako bezpečnostní událost, která může způsobit bezpečnostní incident:

- **Volně dostupné a komerční VPN**: Všechny VPN služby, mimo VPN koncentrátor JU. Uživatelé musí pro vzdálený přístup k univerzitním službám používat pouze oficiální univerzitní VPN.
- **Proxy servery**: Veřejné nebo komerční proxy servery a nástroje umožňující změnu IP adresy.
- **Anonymizační webové prohlížeče**: Prohlížeče jako TOR, I2P a další nástroje pro anonymní přístup k internetu.
- **Jiné anonymizační technologie**: Jakýkoli nástroj nebo technologie, která má za cíl skrýt skutečnou identitu nebo polohu uživatele při připojování k internetu.

V případě detekce použití některých z těchto služeb při navázání spojení se službami JU bude uživatelovi zablokován přístup a resetované heslo pro zamezení zneužití případného útočníka.

c) Doporučení od manažera KB a správců M365 JU.

Doporučujeme, před přístupem k jakékoli službě JU a službám M365, vypínat prostředky anonymizace. Vypnutím těchto nástrojů zamezíte zbytečným resetům hesel na vašem účtu a dalším potenciálním problémům, co mohou z anonymizace nastat.

Pro vylepšení bezpečnosti vašeho univerzitního účtu a zamezení vytváření falešně pozitivních bezpečnostních události dále také doporučujeme si zavést více faktorové ověřování (MFA)[1] pro váš účet.

Pro bezpečné oddělení práce/studia a volného surfování po internetu s anonymizací je možné využít kontejnerizační nástroje zabudované ve webových prohlížečích.

- Mozilla Firefox
    - https://support.mozilla.org/cs/kb/jak-pouzivat-kontejnery-firefoxu
- Prohlížeče na bázi Chromium (Google Chrome, Microsoft Edge, …) a prohlížeč Safari
    - Možné pouze skrze přepínání uživatelských profilů v prohlížeči
    - Návody naleznete na stránkách poskytovatele webových prohlížečů

V případě potřeby zajištění bezpečného připojení do sítě JU na veřejných sítích nebo ze zahraničí využijte VPN koncentrátor JU[2].

[1] Nastavení MFA: https://wiki.jcu.cz/Microsoft_365/MFA

[2] Nastavení VPN: https://wiki.jcu.cz/VPN

Informační sdělení

Ochrana osobního soukromí je v dnešní době velmi důležité a často debatované téma. Pro zajištění co nejvyšší úrovně soukromí je možné využít nespočet nástrojů, služeb nebo i zásad a pravidel, které nám pomohou se snížením naší digitální stopy na internetu. Mezi takové nástroje a služby spadají i proxy servery a VPN nebo například webový prohlížeč TOR.

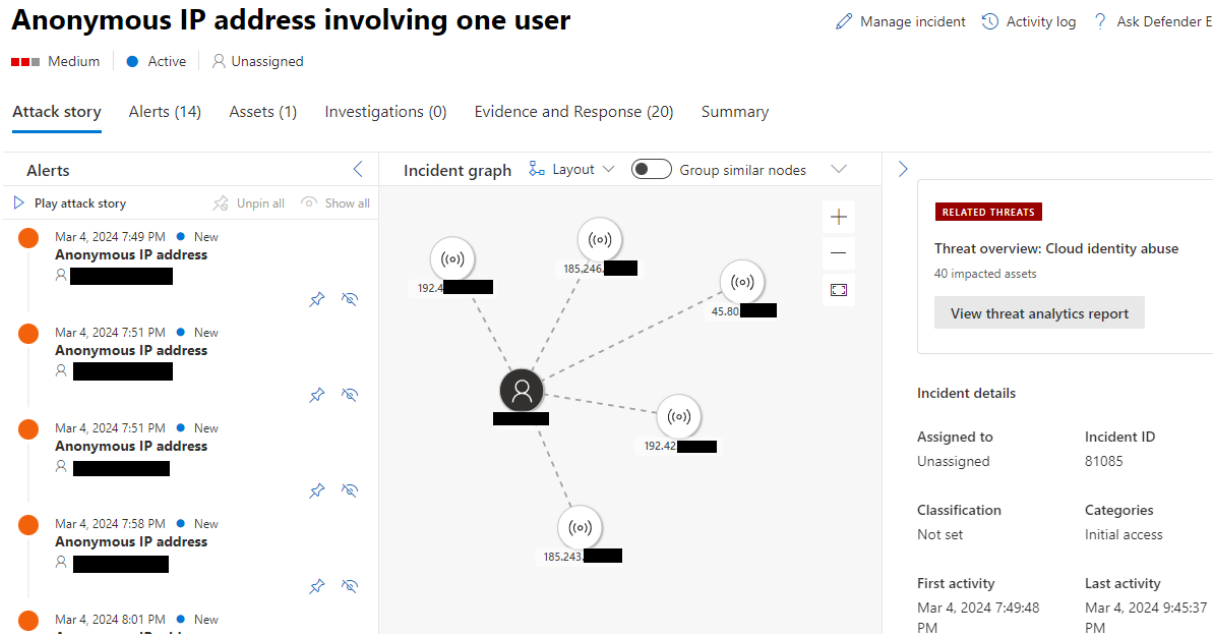
a) Problematika s prostředky anonymizace

Cíl těchto nástrojů je jasný. Kompletně anonymizovat (u VPN někdy i šifrovat) internetový provoz uživatele a zamezit tak sledování od poskytovatele internetu nebo jiných společností. Toto platí pouze do doby, než se uživatel přihlásí **do jakékoli** služby. V okamžiku přihlášení je anonymizace **anulována** a poskytovatel patřičné služby ví o koho se jedná.

Další problém je **časté přepínání lokalit anonymních bodů**, který se využívají pro navázání spojení mezi uživatelem a cílem – zprostředkovatel proxy/VPN. Toto se velice často vyskytuje u volně dostupných proxy serverů a VPN, které nabízí tzv. „free“ servery, ale také u placených služeb, pro zajištění lepší. Z tohoto konstantního přepínání lokalit vzniká ale problém, kdy se v mnoha službách toto chování jeví jako známka útoku a velmi často končí zablokováním účtu.

b) Aktuální stav na JU

Na JU sledujeme nárůst výše zmíněných událostí s častým přepínáním lokalit nebo náhodné připojování z jiných kontinentů světa. Obojí se správně, z bezpečnostního hlediska, automaticky vyhodnocují jako útok – viz obrázek níže.



Obrázek 1: Vyhodnocení bezpečnostní události

Zde byl legitimní uživatel **vyhodnocen jako útočník** díky **přepínání lokalit**. V rámci přibližně 10 minut se uživatel **připojil z několika IP adres** do služby M365, které toto okamžitě hlásí našim specialistům na JU jako útok. Útoky na stejném principu sledujeme i z kompromitovaných účtů na JU, které zneužívají útočníci.